Exploração POC e análise técnica publicada para a Apple 0 dias de vulnerabilidade

Data: 2025-08-25 04:52:54

Autor: Inteligência Against Invaders

Uma vulnerabilidade crítica de execução de código remoto de clique zero no iOS da Apple foi divulgado com uma exploração de prova de conceito de trabalho, marcando outra falha de segurança significativa nos recursos de processamento de imagem da empresa.

A vulnerabilidade, rastreada ASCVE-2025-43300, afeta a implementação da Apple do código de descompressão sem perda JPEG usado no processamento de formato de arquivo DNG (Digital Negative) da Adobe.

Os detalhes da vulnerabilidade

O pesquisador de segurança b1n4r1b01has publicou etapas detalhadas de análise técnica e reprodução para essa exploração de dia zero, que tem como alvo os dispositivos iOS 18.6.1 por meio de arquivos de imagem DNG de maneira maliciosamente criada.

A vulnerabilidade reside no Apple'sRawcamera.bundle, um componente responsável pelo processamento de vários formatos de imagem bruta, incluindo a especificação DNG da Adobe.

A questão principal decorre da amíscia entre as declarações de metadados e o conteúdo de dados reais em arquivos DNG.

Especificamente, a vulnerabilidade é acionada quando um arquivo DNG declara que contém 2 amostras por pixel em seus metadados de subifd (samplesperpixel = 2) enquanto os dados sem perda JPEG incorporados contêm apenas 1 componente em seu marcador SOF3 (início do quadro 3).

Essa inconsistência faz com que a rotina de descompressão execute a gravação de anúncios, potencialmente permitindo que os invasores executem o código arbitrário.

A exploração de prova de conceito demonstra uma compreensão sofisticada das especificações do formato de arquivo TIFF e JPEG. O pesquisador modificou bytes específicos em um arquivo DNG legítimo de uma galeria de amostra Pentax K-3 Mark III:

- Offset 0x2fd00: alterado de 0x01 para 0x02 (modificando os metadados do samplesPerpixel)
- Offset 0x3e40b: alterado de 0x02 para 0x01 (contagem de componentes SoF3 alterando)

Essas modificações mínimas criam as condições precisas necessárias para acionar a vulnerabilidade durante a geração automática de visualização de imagem.

A exploração pode ser entregue através de vários vetores, incluindo airdrop, iMessage ou anexos de email, tornando -o particularmente perigoso, pois não requer interação do usuário além de receber o arquivo malicioso.

Impacto técnico e escopo

O que torna a CVE-2025-43300 particularmente preocupante é a natureza de cliques de zero. O iOS processa automaticamente os arquivos DNG ao gerar visualizações, o que significa que os dispositivos podem ser comprometidos simplesmente recebendo um arquivo de imagem malicioso.

A vulnerabilidade afeta o iOS 18.6.1 e as versões potencialmente anteriores, embora o pesquisador observe que o iOS 18.6.2 parece ter abordado o problema.

O componente Rawcamera.bundle foi despojado de símbolos de depuração, tornando a engenharia reversa desafiadora, mas não impossível.

Essa ofuscação deliberada sugere que a Apple reconhece a natureza sensível desse caminho de código, mas ainda continha uma vulnerabilidade crítica que escapou da detecção durante o desenvolvimento e o teste.

Após a divulgação, a Segurança Researcher matt Suiche desenvolveu o Bouncer, uma ferramenta de detecção baseada em ferrugem de código aberto projetado especificamente para identificar as tentativas de exploração CVE-2025-43300. A ferramenta implementa um algoritmo sofisticado que:

1. Paresia estruturas de arquivos TIFF/DNG com manuseio de endianness adequado
2. Identifica subifds contendo dados compactados sem perdas JPEG
3. Valida a consistência entre as declarações de metadados e dados JPEG reais
4. Arquivos de sinalizadores exibindo as condições específicas de incompatibilidade que acionam a vulnerabilidade

A Apple tem [segundo](#) Abordou essa vulnerabilidade INIOS 18.6.2, embora a empresa não tenha emitido um aviso oficial de segurança no momento desta análise.

A falta de comunicação formal da Apple sobre esse dia zero é preocupante, principalmente devido à gravidade e à disponibilidade de trabalho de exploração de trabalho.

As organizações e os profissionais de segurança são aconselhados a:

- Imediatamente UpdateAll iOS dispositivos para a versão 18.6.2 ou posterior quando disponíveis
- Implementar a validação de arquivos antes do processamento de arquivos DNG em aplicativos personalizados
- Implantar ferramentas de detecção como segurança elegante para identificar possíveis tentativas de exploração
- Considere a visualização de imagem desativada para fontes não confiáveis, sempre que possível

O CVE-2025-43300 representa uma continuação dos desafios contínuos da Apple com a segurança do processamento de imagens. A vulnerabilidade destaca como a complexidade dos formatos de

arquivos modernos, principalmente quando vários padrões interagem (contêineres TIFF com dados JPEG), podem criar superfícies de ataque inesperadas.

Essa divulgação também ressalta a importância crítica das estratégias de defesa em profundidade e o valor da pesquisa de segurança independente na identificação de vulnerabilidades que podem ter sido perdidas durante os processos de teste de fornecedores.

Encontre esta notícia interessante! Siga -nos [Google News](#) Assim, [LinkedIn](#) [X](#) Para obter atualizações instantâneas!